REMARKS

Reconsideration of this Application is respectfully requested. In response to the Office Action mailed July 25, 2005, Applicant has amended claim 1, 2, 4-7, 9-16, 18, 20, 21, and 24. Claims 1-27 are pending.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Request for Acknowledgement of Figures

In the Preliminary Amendment filed September 24, 2002, Applicant submitted new figures 1-6 replacing the figures as filed. Applicant respectfully requests that the Examiner consider these figures.

Power of Attorney

Applicant respectfully requests entry of the Power of Attorney filed June 27, 2005.

Rejections under 35 U.S.C. § 112

On pages 2-3, the Action rejects claims 21-27 under 35 U.S.C. § 112, second paragraph, alleging these claims are "indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention." The Action provides two reasons in support of the rejection.

First, the Action alleges the "term 'approximately' in claim 21 is a relative term which renders the claim indefinite." Accordingly, the term "approximately" has been cancelled from the claim. Therefore, the claim rejection is rendered moot.

Second, the Action alleges the claim element "'the first and second encryption keys . . . being other than modifiable absent erasing thereof by any code other than the program code' is unclear, particularly 'absent erasing thereof.'"

Applicant has amended claim 21 to recite "the first and second super-root keys being accessible only by the program code and being modifiable only by the program code for all modifications excluding erasure." Applicant contends that this clarifies claim 21. Accordingly, Applicant respectfully requests that the rejection be withdrawn.

Rejections under 35 U.S.C. § 103

I. On pages 3-5, the Action rejects claims 1-9 and 15-18 under 35 U.S.C. § 103(a) as being unpatentable over Applied Cryptography, Second Edition to Schneier (hereinafter "Schneier") in view of U.S. Patent No. 6,175,924 to Arnold (hereinafter "Arnold"), in further view of U.S. Patent No. 6,141,423 to Fischer (hereinafter "Fischer"). Applicant respectfully traverses this rejection.

(A) On pages 3-4, the Action rejects claim 1. Amended claim 1 recites: "A method for transferring **a first root key** between a key provider system and a second other system via an information network comprising the steps of: a) encrypting the first root key using **a first super-root key** of the key provider; b) providing within the second other system a first secure module having a second super-root key within a read-only memory circuit thereof and provided with the first secure module, the second super-root key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second super-root key is other than modifiable and other than accessible outside of the module; c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored within the read-only memory circuit of the first secure module and to store the decrypted first root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting **private keys**, and wherein a bit length of the first super-root key is **greater than** a bit length of the first root key, and said bit length of the first root key is **greater than** a bit length of any of said private keys." (Emphasis added.)

For at least the following two reasons, the combined teachings of Schneier, Arnold, and Fischer do not establish a *prima facie* case of obviousness to reject amended claim 1.

First, Schneier, Arnold, and Fischer do not teach or suggest a relationship between a bit length for multiple keys. Specifically, Schneier, Arnold, and Fischer do not teach or suggest "wherein a bit length of the first super-root key is **greater than** a bit length of the first root key, and said bit length of the first root key is **greater than** a bit length of any of said private keys," as recited in claim 1. Schneier only discloses two types of keys: Key-Encryption Keys and Data Keys, and therefore does not teach a relationship between bit lengths of three keys (see Scheier, page 176). Arnold only discloses two types of keys: the private key K_{PR} and the public key K_{PU}, and thus does not teach a relationship between bit lengths of three keys (see Arnold, col. 5, lines 31-38). Fischer discloses a private key, a random DES key, a public key, and a trustee's public key (see Fischer, col. 4, lines 59-61, col. 7, lines 28-33, col. 9, lines 58-60). However, Fischer does not teach or suggest a relationship between the bit lengths of any of the keys. Thus, Schneier, Arnold, and Fischer do not teach or suggest "wherein a bit length of the first super-root key is **greater than** a bit length of the first root key, and said bit length of the first root key is **greater than** a bit length of any of said private keys," as recited in claim 1.

Second, Schneier, Arnold, and Fischer do not teach or suggest the claimed relationship between the "first root key," the "first super-root key," and the "private encryptions keys." Specifically, Schneier, Arnold, and Fischer do not teach or suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 1. Schneier only discloses two types of keys: Key-Encryption Keys and Data Keys, and therefore does not teach a relationship between three keys (see Schneier, page 176). Arnold only discloses two types of keys: the private key K_{PR} and the public key K_{PU}, and thus does not teach a relationship between three keys (see Arnold, col. 5, lines 31-38). Fischer discloses a private key, a random DES key, a public key, and a trustee's public key (see Fischer, col. 4, lines 59-61, col. 7, lines 28-33, col. 9, lines 58-60). However, Fischer does not teach or suggest encrypting the random DES key with the public key, transferring the encrypted random DES key to a key provider to a second system via an information network, and using the random DES key for encrypting and decrypting the private key. Thus, Schneier, Arnold, and Fischer do not teach or suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root**

key is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 1. Therefore, claim 1 is allowable over the combined teachings of Schneier, Arnold, and Fischer and allowance thereof is respectfully requested.

Claims 2-9, which depend from claim 1, are also in condition for allowance due to their dependence on an allowable claim.

(B) Claim 15 is allowable for reasons analogous to those given for claim 1.

Claims 16-18, which depend from claim 15, are also in condition for allowance due to their dependence on an allowable claim.

II. On pages 5-7, the Action rejects claims 10-14 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Fischer, and Arnold, in further view of U.S. Patent No. 5,680,458 to Spelman et al. (hereinafter "Spelman").

On pages 5-6, the Action rejects claim 10. Claim 10 is allowable for reasons analogous to those given for claim 1.

Claims 11-14, which depend from claim 10, are also in condition for allowance due to their dependence on an allowable claim.

III. On pages 7-8, the Action rejects claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Fischer, and Arnold, in further view of U.S. Patent No. 5,559,889 to Easter et al. (hereinafter "Easter").

Claim 19 depends from allowable claim 15, and is therefore in condition for allowance due to its dependence on an allowable claim.

IV. On page 8, the Action rejects claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Fischer, and Easter, in further view of U.S. Patent No. 5,249,277 to Bergum et al. (hereinafter "Bergum").

Claim 20 depends from allowable claim 15, and is therefore in condition for allowance due to its dependence on an allowable claim.

V. On page 9, the Action rejects claims 21-24 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Fischer, and Spelman, in further view of U.S. Patent No. 6,331,784 to Mason et al. (hereinafter "Mason").

Claim 21 is allowable for reasons analogous to those given for claim 1.

Claims 22-24, which depend from allowable claim 21, are also in condition for allowance because of their dependence on an allowable claim.

VI. On pages 9-10, the Action rejects claim 25 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Fischer, Mason and Spellman, in further view of U.S. Patent No. 4,386,234 to Ehrsam et al. (hereinafter "Ehrsam").

Claim 25 depends from allowable claim 21, and is therefore in condition for allowance due to its dependence on an allowable claim.

VII. On pages 10-11, the Action rejects claim 26 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Spellman, Fischer, Mason, and Ehrsam, in further view of Easter.

Claim 26 depends from allowable claim 21, and is therefore in condition for allowance due to its dependence on an allowable claim.

VIII. On page 11, the Action rejects claim 27 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Fischer, Spelman, Mason, Ehrsam, and Easter, in further view of Bergum.

Claim 27 depends from allowable claim 21, and is therefore in condition for allowance due to its dependence on an allowable claim.

Therefore, claims 1-27 are in condition for allowance and allowance thereof is respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment is respectfully requested.

Respectfully submitted,

Date Nov. 14, 2005

Edward W. Yee
Registration No. 47,294
VENABLE, LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300